

Publicacions Matemàtiques, Vol **42** (1998), 119–130.

ON THE p -RANK OF AN ABELIAN VARIETY AND ITS ENDOMORPHISM ALGEBRA

JOSEP GONZÁLEZ

Abstract

Let A be an abelian variety defined over a finite field. In this paper, we discuss the relationship between the p -rank of A , $r(A)$, and its endomorphism algebra, $\text{End}^0(A)$. As is well known, $\text{End}^0(A)$ determines $r(A)$ when A is an elliptic curve. We show that, under some conditions, the value of $r(A)$ and the structure of $\text{End}^0(A)$ are related. For example, if the center of $\text{End}^0(A)$ is an abelian extension of \mathbb{Q} , then A is ordinary if and only if $\text{End}^0(A)$ is a commutative field. Nevertheless, we give an example in dimension 3 which shows that the algebra $\text{End}^0(A)$ does not determine the value $r(A)$.

1. Introduction

Let k be an algebraically closed field of characteristic $p > 0$. Given an abelian variety A/k of dimension g , the p -rank of A is defined by

$$r(A) := \dim_{\mathbb{F}_p} \text{Pic}^0(A)[p] = \dim_{\mathbb{F}_p} H^1(A, \mathcal{O})^{\mathbb{F}^*},$$

where F^* denotes the absolute Frobenius. The value $r(A)$ is invariant under isogenies and satisfies $r(A \times B) = r(A) + r(B)$, for A, B abelian varieties over k . Thus, if A is isogenous to a product of abelian varieties $\prod_{i=1}^m A_i^{n_i}$, then $r(A) = \sum_{i=1}^m n_i r(A_i)$.

Let \mathcal{C}/k be a non-singular projective curve of genus $g > 0$. Serre [Se 58] characterized the Hasse-Witt invariant, $r(\mathcal{C})$, by means of the action of F^* on the first cohomology group:

$$r(\mathcal{C}) = \dim_{\mathbb{F}_p} H^1(\mathcal{C}, \mathcal{O})^{F^*}.$$

This research has been partially supported by DGICYT, PB-93-0034.

If J denotes the jacobian of \mathcal{C} , it is clear that $r(J) = r(\mathcal{C})$. Ordinary abelian varieties are those for which $r(A) = g$. Supersingular elliptic curves are those for which $r(A) = 0$.

Let us denote by $\text{End}^0(A) := \mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(A)$ the endomorphism algebra of A . If E/k is an elliptic curve, E is ordinary if and only if $\text{End}^0(E)$ is a commutative field (it is equal to \mathbb{Q} or to an imaginary quadratic extension of \mathbb{Q}); E is supersingular if and only if $\text{End}^0(E)$ is a quaternion algebra over \mathbb{Q} . If, in addition, the field k is the algebraic closure of a finite field, the case $\text{End}^0(E) = \mathbb{Q}$ is excluded.

The asymptotic behaviour of the Hasse-Witt invariants for the fibres of modular curves, resp. of Fermat curves, has been studied in [Ba-Go 97], resp. [Go 97]. Both cases are quite different. It turns out that, for some projective curves over \mathbb{Q} , the distribution of the extreme values of the Hasse-Witt invariant of the fibres seems to depend on the type of the endomorphism algebra over $\overline{\mathbb{Q}}$ of their jacobian variety.

In this paper, we summarize some results which show the relationship between $r(A)$ and $\text{End}^0(A)$ when the abelian variety A is defined over a finite field. Nevertheless, we provide with an example of two abelian varieties which have \mathbb{Q} -isomorphic endomorphism algebras but show different p -ranks. One of them is the jacobian of the modular curve $X_0(41)/\mathbb{F}_3$.

Some of these results are contained in my PhD thesis. I would like to finish this introduction by expressing my gratitude to my dissertation advisor Prof. Pilar B  yer for her help and encouragement throughout the realization of the work.

2. Some general facts

We fix a positive integer n and consider a power $q = p^n$ of the characteristic of k . Throughout, A denotes an abelian variety of dimension $g > 0$ defined over the finite field \mathbb{F}_q , and $k = \overline{\mathbb{F}}_q$. We denote by $\text{End}_{\mathbb{F}_q}(A)$, resp. $\text{End}(A)$, the ring of endomorphisms of A which are defined over \mathbb{F}_q , resp. k . We write $\text{End}_{\mathbb{F}_q}^0(A) := \mathbb{Q} \otimes_{\mathbb{Z}} \text{End}_{\mathbb{F}_q}(A)$, $\text{End}^0(A) := \mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(A)$. If A is \mathbb{F}_q -isogenous to $\prod A_i^{n_i}$, where the abelian varieties A_i are \mathbb{F}_q -simple and not \mathbb{F}_q -isogenous to each other, then $\text{End}_{\mathbb{F}_q}^0(A) = \oplus M_{n_i}(\text{End}_{\mathbb{F}_q}^0(A_i))$, where M_{n_i} denotes the ring of $(n_i \times n_i)$ -matrices.

Let $\varphi \in \text{End}_{\mathbb{F}_q}(A)$ be the relative Frobenius endomorphism, whose action on the variety raises to the q -th power the coordinates of the points of A . For a given prime number $\ell \neq p$, we denote by $T_\ell(A)$ the Tate module of A , and by $V_\ell(A) := \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(A)$. Two abelian varieties A, B defined

over \mathbb{F}_q are \mathbb{F}_q -isogenous if and only if the corresponding Frobenius have the same characteristic polynomial in the ℓ -adic representation.

The \mathbb{Q} -algebra $\text{End}_{\mathbb{F}_q}^0(A)$ has $\mathbb{Q}(\varphi)$ as its center. We have that $\text{End}_{\mathbb{F}_q}^0(A) = \mathbb{Q}(\varphi)$ if and only if the characteristic polynomial of φ acting on the Tate module has no double roots. We have that $\mathbb{Q}(\varphi) = \mathbb{Q}$ if and only if A is \mathbb{F}_q -isogenous to the g -th power of a supersingular elliptic curve with all its endomorphisms defined over \mathbb{F}_q . All these assertions can be found in [Ta 66].

Given an \mathbb{F}_q -polarization $\lambda : A \rightarrow \widehat{A}$, we consider the Rosati involution, defined on $\text{End}^0(A)$ by $\psi \mapsto \psi' = \lambda^{-1} \circ \widehat{\psi} \circ \lambda$. It belongs to $\mathbb{Q}(\varphi)$. The *Verschiebung*, φ' , is an element of $\text{End}_{\mathbb{F}_q}(A)$ and satisfies $\varphi \circ \varphi' = q$.

If A is \mathbb{F}_q -simple, then $\mathbb{Q}(\varphi)$ is a number field and the Rosati involution agrees on $\mathbb{Q}(\varphi)$ with the complex conjugation c , for all embeddings of $\mathbb{Q}(\varphi)$ into $\overline{\mathbb{Q}}$. The class in the Brauer group of $\mathbb{Q}(\varphi)$ of the simple algebra $\text{End}_{\mathbb{F}_q}^0(A)$ is characterized by the local invariants $i_\varphi = f_\varphi \text{ord}_\varphi(\varphi)/n$ at each prime φ over p in $\mathbb{Q}(\varphi)$ (here, f_φ stands for the residual degree at φ); on each real prime, the local invariant is equal to $1/2$; on the remaining primes, the algebra splits. The lowest common denominator e of all the invariants i_φ is the period of the endomorphism algebra $\text{End}_{\mathbb{F}_q}^0(A)$. The characteristic polynomial of φ acting on the Tate module equals the e -th power of the \mathbb{Q} -irreducible polynomial of φ (cf. [Ta 66], [Wa 69]).

We fix an algebraic closure $\overline{\mathbb{Q}}$ of \mathbb{Q} . An element $\alpha \in \overline{\mathbb{Q}}$ is called a Weil q -number if $|\alpha| = q^{1/2}$, for all archimedean absolute values $|\cdot|$ on $\overline{\mathbb{Q}}$. Each Weil q -number α determines, up to isogenies, an \mathbb{F}_q -simple abelian variety A/\mathbb{F}_q such that the \mathbb{Q} -irreducible polynomial of φ equals the \mathbb{Q} -irreducible polynomial of α . This assignment establishes a one to one correspondence between the conjugation classes of Weil q -numbers and the \mathbb{F}_q -isogenies classes of \mathbb{F}_q -simple abelian varieties which are \mathbb{F}_q -defined (cf. [Ta 68]).

Let α_1, α_2 be two Weil q -numbers such that $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$. If the ideals $(\alpha_1), (\alpha_2)$ in the ring of integers of $K := \mathbb{Q}(\alpha_1)$ coincide, then their associated abelian varieties are $\overline{\mathbb{F}}_q$ -isogenous. If $(\alpha_1) = (\alpha_2)$, then there exists a unit $\varepsilon \in K$ such that $\alpha_2 = \varepsilon \alpha_1$; since $|\varepsilon| = 1$, we have that ε must be a root of unity. If $\varepsilon^s = 1$, then $\alpha_1^s = \alpha_2^s$. The characteristic polynomials of the relative Frobenius of both abelian varieties over \mathbb{F}_{q^s} are equal. Thus, the varieties are \mathbb{F}_{q^s} -isogenous. We note that the abelian variety associated to a Weil q -number α is $\overline{\mathbb{F}}_q$ -isogenous to a power of a supersingular elliptic curve if and only if the ideals (α^2) and (q) do coincide.

In the sequel the term *isogenous* will indicate $\overline{\mathbb{F}}_q$ -isogenous.

3. Some relations between $\text{End}^0(A)$ and $r(A)$

In this section we give some propositions which relate the p -rank $r(A)$ to the structure of the \mathbb{Q} -algebra $\text{End}_{\mathbb{F}_q}^0(A)$.

Let $P(X) := \det(\varphi - X \text{Id} \mid V_\ell(A))$, which is a polynomial with integer coefficients independent of ℓ . If α_i , $1 \leq i \leq g$, denote its complex roots, then we have that $|\alpha_i| = q^{1/2}$ and $\prod_{i=1}^{2g} \alpha_i = q^g$. The real roots of $P(X)$ have even multiplicity and we can order all the roots so that $\alpha_{i+g} = \bar{\alpha}_i = q/\alpha_i$, for $1 \leq i \leq g$. For such an order we write $\beta_i := \alpha_i + q/\alpha_i$. The polynomial $Q(X) := \prod_{i=1}^g (X - \beta_i)$ has integer coefficients too. We have

$$Q(X)^2 = \det(\varphi + \varphi' - X \text{Id} \mid V_\ell(A)), \quad P(X) = X^g Q\left(X + \frac{q}{X}\right).$$

Then $P(X)(\text{mod } p) = X^g Q(X)(\text{mod } p)$. The following results are known (cf. [Ma 65], [St 79], [Ba-Go 97]).

3.1. Proposition.

- i) $r(A)$ is the sum of the multiplicities of the non-zero roots of the $(\text{mod } p)$ -reduced characteristic polynomial $P(X)$ and, hence, of those of the polynomial $Q(X)(\text{mod } p)$.
- ii) We have $r(A) = \#\{\beta_i \notin \wp \mid 1 \leq i \leq g\} = \#\{\alpha_i \notin \wp \mid 1 \leq i \leq 2g\}$, where \wp is a prime ideal over p in the ring of integers of $\mathbb{Q}(\{\alpha_i\})$.

By using the results displayed in the proposition and in the previous section, we obtain

3.2. Proposition. Let A/\mathbb{F}_q be an \mathbb{F}_q -simple abelian variety. Then:

- i) A is ordinary if and only if the ideals (φ) , (φ') (equivalently, the ideals $(\varphi + \varphi')$, (p)) are relatively prime in $\mathbb{Q}(\varphi)$.
- ii) $r(A) = 0$ if and only if every prime $\wp \mid (p)$ divides (φ) in $\mathbb{Q}(\varphi)$ (equivalently, divides $(\varphi + \varphi')$).
- iii) A is isogenous to a power of a supersingular elliptic curve if and only if $(\varphi) = (\varphi')$.
- iv) The period e of $\text{End}_{\mathbb{F}_q}^0(A)$ in the Brauer group divides $r(A)$.

From now on, we assume that A/\mathbb{F}_q is \mathbb{F}_q -simple. As usual, we will say that A is absolutely simple if it is k -simple.

3.3. Corollary. *If there exists a prime ideal $\wp \mid (p)$ such that $\wp^c = \wp$, then A is non ordinary. If A is not isogenous to a power of a supersingular elliptic curve, then there exists a prime ideal $\wp \mid (p)$ such that $\wp \neq \wp^c$.*

Proof: Since $\varphi^c = \varphi'$, if $\wp = \wp^c$ we shall have $\wp \mid (\varphi + \varphi')$ and A will be non ordinary. If every prime ideal over p is invariant under complex conjugation, then $(\varphi) = (\varphi')$. ■

3.4. Proposition. *Assume that $q = p$. Then, we have*

- i) *If A is non ordinary, there exists a prime $\wp \mid (p)$ in $\mathbb{Q}(\varphi)$ which ramifies.*
- ii) *If $r(A) = 0$, every prime $\wp \mid (p)$ in $\mathbb{Q}(\varphi)$ does ramify.*
- iii) *$\text{End}_{\mathbb{F}_p}^0(A)$ is a totally imaginary number field if and only if A is not isogenous to the square of a supersingular elliptic curve.*

Proof: If A is non ordinary there exists a prime $\wp \mid (p)$ such that $\wp \mid (\varphi)$ and $\wp \mid (\varphi')$. Since $\varphi\varphi' = p$, it follows that \wp ramifies. If $r(A) = 0$, the condition is fulfilled by all the primes which divide (p) . Let us prove iii). We recall that A is \mathbb{F}_p -simple. Since $n = 1$, the period e in the Brauer group is 1 or 2, depending on whether $\mathbb{Q}(\varphi)$ is totally imaginary or not. Thus, $e = 1$ if and only if $\text{End}_{\mathbb{F}_p}^0(A)$ is a totally imaginary number field. The value e is equal to 2 if and only if $\varphi^2 = p$. In this case, the characteristic polynomial of φ is $(X^2 - p)^2$, which has associated an \mathbb{F}_p -simple abelian variety \mathbb{F}_{p^2} -isogenous to the square of a supersingular elliptic curve defined over \mathbb{F}_{p^2} . ■

3.5. Proposition. *If $r(A)$ is prime to g , then $\text{End}_{\mathbb{F}_q}^0(A)$ is a commutative field.*

Proof: If $\dim A = 1$, the statement is known and, therefore, we may assume that $g > 1$. The field $\mathbb{Q}(\varphi)$ is either totally imaginary, equal to $\mathbb{Q}(\sqrt{p})$, or equal to \mathbb{Q} . Since A is \mathbb{F}_q -simple, the last possibility is excluded in our case. Thus $[\mathbb{Q}(\varphi) : \mathbb{Q}]$ is even and e divides g , because $e[\mathbb{Q}(\varphi) : \mathbb{Q}] = 2g$. Since e also divides $r(A)$, it follows that $e = 1$. ■

The following theorem allows us to characterize, by means of the commutativity of $\text{End}^0(A)$, the ordinary character of those absolutely simple

abelian varieties whose \mathbb{Q} -algebra $\text{End}^0(A)$ has as center an abelian extension of \mathbb{Q} . Note that, since the center of the endomorphism algebra of an elliptic curve is always abelian over \mathbb{Q} , the ordinary character of an elliptic curve, E , is equivalent to the commutativity of $\text{End}^0(E)$.

3.6. Theorem.

- i) *If A is ordinary, then $\text{End}_{\mathbb{F}_q}^0(A)$ is commutative and, therefore, $\text{End}_{\mathbb{F}_q}^0(A) = \mathbb{Q}(\varphi)$. In particular, if A is ordinary and absolutely simple, $\text{End}^0(A)$ is commutative.*
- ii) *If p splits completely in $\mathbb{Q}(\varphi)$ and $\text{End}_{\mathbb{F}_q}^0(A)$ is commutative, then A is ordinary.*
- iii) *If A is absolutely simple and the center K of $\text{End}^0(A)$ is an abelian extension of \mathbb{Q} , then p splits completely in K .*

Proof: i) Let us assume that A is ordinary. The ideals (φ) , (φ') are relatively prime in $\mathbb{Q}(\varphi)$ by 3.2 i) and $\varphi\varphi' = p^n$. Thus, for all primes $\wp \mid (p)$ in $\mathbb{Q}(\varphi)$, we have that $\text{ord}_{\wp}\varphi$ is zero or a positive multiple of n and, so, $i_{\wp} \in \mathbb{Z}$. The field $\mathbb{Q}(\varphi)$ has no real primes, because if φ were real, then $\varphi = \pm q^{1/2}$ and A would be non ordinary. Since all the local invariants of $\text{End}_{\mathbb{F}_q}^0(A)$ are trivial, its Brauer period must be $e = 1$; i.e., $\text{End}_{\mathbb{F}_q}^0(A) = \mathbb{Q}(\varphi)$. This line of reasoning parallels that used in [Yu 78] for the case of the jacobian of a curve.

Let us now prove ii). If $\text{End}_{\mathbb{F}_q}^0(A)$ is commutative and p splits completely, then for all primes $\wp \mid (p)$ in $\mathbb{Q}(\varphi)$ we have $i_{\wp} = \text{ord}_{\wp}\varphi/n \in \mathbb{Z}$ and $\text{ord}_{\wp}\varphi$ is zero or n . Since $n = \text{ord}_{\wp}\varphi + \text{ord}_{\wp}\varphi'$, we get that (φ) and (φ') are relatively prime and A is ordinary.

Let us see iii). We may assume without loss of generality that $\text{End}^0(A)$ is equal to $\text{End}_{\mathbb{F}_q}^0(A)$. Then $K = \mathbb{Q}(\varphi^s)$, for all $s > 0$. The \mathbb{Q} -irreducible polynomial of φ is $\prod_{\sigma \in G} (X - \sigma(\varphi))$, where $G = \text{Gal}(K/\mathbb{Q})$. Let $\wp \mid (p)$ be a prime in K and let \mathcal{D} denote its decomposition group in K/\mathbb{Q} . Assume that p does not split completely in K . Then we can take $\sigma \in \mathcal{D} \setminus \{\text{Id}\}$ and the ideals $(\sigma(\varphi))$ and (φ) coincide, since K/\mathbb{Q} is abelian. There exists a root of unity $\varepsilon \in K$ such that $\varphi = \varepsilon\sigma(\varphi)$. If $s > 1$ is the order of ε , then $\varphi^s = \sigma(\varphi^s)$. Then $[\mathbb{Q}(\varphi^s) : \mathbb{Q}] < [\mathbb{Q}(\varphi) : \mathbb{Q}]$, which is a contradiction. ■

If A/\mathbb{F}_q and B/\mathbb{F}_q are absolutely simple abelian varieties of dimension $g > 1$, then A and B can have \mathbb{Q} -isomorphic endomorphism algebras by means of a homomorphism $\Phi : \text{End}^0(A) \xrightarrow{\sim} \text{End}^0(B)$ such that $\Phi(\varphi_A)$ is none of the conjugates of φ_B . If this is the case, A and B are not \mathbb{F}_q -isogenous. Nevertheless, as the following theorem shows, they have the same p -rank when $g = 2$.

3.7. Theorem. *Let A/\mathbb{F}_q be an absolutely simple abelian variety of dimension $g < 3$. We have*

- i) *If $g = 1$, then $\text{End}^0(A)$ determines A up to isogenies.*
- ii) *If $g = 2$, then $\text{End}^0(A)$ is a commutative field which determines $r(A)$. If, moreover, p does not split completely in $\text{End}^0(A)$, then $\text{End}^0(A)$ determines A up to isogenies.*

Proof: The assertion i) is well known. We assume, without loss of generality, that $\text{End}^0(A) = \text{End}_{\mathbb{F}_q}^0(A)$. Thus, $\mathbb{Q}(\varphi)$ is the center of $\text{End}^0(A)$.

For all abelian varieties A/\mathbb{F}_q of dimension 2 the condition $r(A) = 0$ is equivalent to the fact that A is isogenous to the square of a supersingular elliptic curve. Thus, if A is absolutely simple, either A is ordinary or $r(A) = 1$.

Assume that $\dim A = 2$ and that A is absolutely simple. Since, in particular, A is not isogenous to a power of a supersingular elliptic curve, the field $K := \mathbb{Q}(\varphi)$ is totally imaginary and the ideals (φ) , (φ') are different, by 3.2 iii).

In order to show that $\text{End}^0(A)$ is a commutative field, we prove that $e = 1$. Since $e[K : \mathbb{Q}] = 4$ and $K \neq \mathbb{Q}$, $e = 2$ or $e = 1$. Assume that $e = 2$. Then $[K : \mathbb{Q}] = 2$ and the prime p splits completely in K by 3.6 iii). We have that $(p) = \wp \wp^c$. The ideal (φ) is $\wp^i(\wp^c)^{n-i}$, for some i such that $0 \leq i \leq n$, and the corresponding local invariants are i/n , $(n-i)/n$. Since $e = 2$, we have that $i = n/2$ and $(\varphi) = (\varphi')$, which leads to a contradiction. Thus, $e = 1$ and $[K : \mathbb{Q}] = 4$.

Let $L := \mathbb{Q}(\varphi + \varphi')$, which is a quadratic extension of \mathbb{Q} . By 3.3, there exists a prime ideal $\wp_1 \mid (p)$ in K such that $\wp_1 \neq \wp_1^c$. This yields the following possibilities for the splitting type of (p) in K :

- a) $(p) = \wp_1^2(\wp_1^c)^2$ $(p \text{ ramifies in } L)$,
- b) $(p) = \wp_1 \wp_1^c$ $(p \text{ is inert in } L)$,
- c) $(p) = \wp_1 \wp_1^c \wp_2^s$, $1 \leq s \leq 2$, $(p \text{ splits completely in } L \text{ and not in } K)$,
- d) $(p) = \wp_1 \wp_1^c \wp_2 \wp_2^c$ $(p \text{ splits completely in } K)$.

In case a), the ideal (φ) is $\wp^i(\wp^c)^{2n-i}$, $0 \leq i \leq 2n$. The local invariants i/n , $(2n-i)/n$ are integers if and only if $i \in \{0, n, 2n\}$. The case $i = n$ is not possible, since (φ) , (φ') would coincide. Thus, (φ) is equal to \wp^{2n} or $(\wp^c)^{2n}$. The two possible ideals are conjugated and, therefore, they correspond to isogenous abelian varieties. Thus, the p -rank of A is determined. In this particular case, A is ordinary, since (φ) and (φ') are relatively prime in K and we apply 3.2 i).

In case b), we have that (φ) is \wp_1^n or $(\wp_1^c)^n$. The two ideals are conjugated and they correspond to isogenous abelian varieties, which are ordinary.

In case c), we have that (φ) is $\wp_1^n \wp_2^{sn/2}$ or $(\wp_1^c)^n \wp_2^{sn/2}$. The two solutions are conjugated and they correspond to isogenous abelian varieties, which are not ordinary because $\wp_2 = \wp_2^c$. Thus $r(A) = 1$.

In case d), the ideal (φ) is equal to $\wp_1^n \wp_2^n$, $\wp_1^n (\wp_2^c)^n$, $(\wp_1^c)^n \wp_2^n$ or $(\wp_1^c)^n (\wp_2^c)^n$. These four solutions correspond to two possible ordinary abelian varieties which are not isogenous.

We see that in all cases $r(A)$ is determined by $\text{End}^0(A)$. If p does not split completely in $\text{End}^0(A)$ then only cases a), b) or c) are possible. In all of them, A is determined up to isogenies by $\text{End}^0(A)$. We remark that the first claim of ii) can be deduced from [Oo 87, 6.5]. ■

If $\dim A = 2$ and A/\mathbb{F}_q is not \mathbb{F}_q -simple, a counting of dimensions in each possible splitting type of A shows that the \mathbb{Q} -algebra $\text{End}^0(A)$ also determines $r(A)$.

4. An example

In this section we will give an example of two absolutely simple abelian varieties of dimension 3 which have isomorphic endomorphism algebras but different p -ranks.

Let α be a Weil q -number. For each positive integer m , we denote by A_m an abelian variety associated to the Weil q^m -number α^m . Let e_m be the Brauer period of $\text{End}_{\mathbb{F}_{q^m}}^0(A_m)$. We have the following equivalent conditions:

- i) A_1/\mathbb{F}_q is absolutely simple.
- ii) A_1/\mathbb{F}_{q^m} is \mathbb{F}_{q^m} -simple for all positive integers m .
- iii) $\dim A_1 = \dim A_m$ for all positive integers m .
- iv) $[\mathbb{Q}(\alpha) : \mathbb{Q}]e_1 = [\mathbb{Q}(\alpha^m) : \mathbb{Q}]e_m$ for all positive integers m .

Since $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a finite extension, there exists a positive integer t such that $\mathbb{Q}(\alpha^t) = \mathbb{Q}(\alpha^{tm})$ for all positive integers m . For this t , we have that $e_t = e_{tm}$ for all m and, thus, A_t is absolutely simple. The abelian variety A_1 is absolutely simple if and only if $\dim A_1 = \dim A_t = [\mathbb{Q}(\alpha^t) : \mathbb{Q}]e_t/2$ and, in this case, we have that $\text{End}^0(A_1) = \text{End}_{\mathbb{F}_{q^t}}^0(A_t)$. In particular, if $\mathbb{Q}(\alpha^m) = \mathbb{Q}(\alpha)$ for all m , then A_1 is absolutely simple and $\text{End}^0(A_1) = \text{End}_{\mathbb{F}_q}^0(A_1)$. This is the condition which we will use in our example.

The next proposition yields a criterion which makes it easy to determine whether an abelian variety A/\mathbb{F}_q , associated to a Weil q -number α such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$, is absolutely simple.

4.1. Proposition. *Let α be a Weil q -number such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. If there exists a positive integer s such that $\mathbb{Q}(\alpha^s) \subsetneq \mathbb{Q}(\alpha)$, then the \mathbb{Q} -irreducible polynomial of α , $P(x)$, is of type $X^6 + aX^3 + q^3$ or $\mathbb{Q}(\alpha) = \mathbb{Q}(\mu_7)$. If the polynomial $P(x)$ is of type $X^6 + aX^3 + q^3$, then $\mathbb{Q}(\alpha^3) \subsetneq \mathbb{Q}(\alpha)$.*

Proof: For each positive integer s , the field $\mathbb{Q}(\alpha^s)$ is real if and only if $\alpha^s = \pm q^{1/2}$. In this case $[\mathbb{Q}(\alpha^s) : \mathbb{Q}]$ is 2 or 1; otherwise, $\mathbb{Q}(\alpha^s)$ is totally imaginary. We write $K := \mathbb{Q}(\alpha)$ and we denote by $L := \mathbb{Q}(\alpha + \bar{\alpha})$ the largest real subfield of K . The field L is the only subfield of K which has dimension 3 over \mathbb{Q} and, thus, $[\mathbb{Q}(\alpha^s) : \mathbb{Q}] \neq 3$ for all positive integers s .

Let m be the smallest positive integer such that $\mathbb{Q}(\alpha^m) \subsetneq K$. The integer m is odd, otherwise $[\mathbb{Q}(\alpha^{m/2}) : \mathbb{Q}] = 6$ and, then $[\mathbb{Q}(\alpha^m) : \mathbb{Q}] = 3$. We consider two cases.

1) The Weil q -number α is equal to $q^{1/2}\zeta$, where ζ is a root of unity.

We assume that $q^{1/2} \in \mathbb{Z}$. Then $K = \mathbb{Q}(\zeta)$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$. Therefore, $K = \mathbb{Q}(\mu_7)$ or $K = \mathbb{Q}(\mu_9)$. If $K = \mathbb{Q}(\mu_9)$, then the polynomial $P(X)$ is equal to $X^6 \pm q^{3/2}X^3 + q^3$.

If $q^{1/2} \notin \mathbb{Z}$ then $\alpha^2 = q\zeta^2$. We have that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$, because $m > 2$, and K is equal to $\mathbb{Q}(\mu_7)$ or $\mathbb{Q}(\mu_9)$. Since m is odd, we have that $q^{m/2} \notin \mathbb{Q}$ and $[\mathbb{Q}(\alpha^m) : \mathbb{Q}] = 2$. The field $\mathbb{Q}(\mu_9)$ only contains the quadratic field $\mathbb{Q}(\sqrt{-3})$. Thus, if $K = \mathbb{Q}(\mu_9)$ then $p = 3$ and $\alpha = \pm(-q)^{1/2}\zeta_1$, where ζ_1 is a primitive 9-th root of unity; in this case, the polynomial $P(x)$ is equal to $X^6 \pm (3q^3)^{1/2}X^3 + q^3$.

2) $\mathbb{Q}(\alpha^s) \neq \mathbb{Q}$ for all positive integers s .

In this case $\mathbb{Q}(\alpha^m)/\mathbb{Q}$ is an imaginary quadratic extension and there exist two primitive m -th roots of unity, ζ_1 and ζ_2 , such that

$$P(X) = (X - \alpha)(X - \alpha\zeta_1)(X - \alpha\zeta_2)(X - \bar{\alpha})(X - \bar{\alpha}\zeta_1^{-1})(X - \bar{\alpha}\zeta_2^{-1}).$$

We denote by \tilde{K} the normal closure of K . We write $G := \text{Gal}(\tilde{K}/\mathbb{Q})$, $H := \{\sigma \in G \mid \sigma(\alpha\zeta_2) = \alpha\zeta_2\}$. We note that if $\sigma(\alpha\zeta_2) = \alpha\zeta_2$ and $\sigma(\alpha\zeta_1) = \alpha\zeta_1$, then $\sigma = \text{Id}$ since the complex conjugation is in the center of G . We consider the following possibilities:

i) $H \neq \{\text{Id}\}$. In this case, there exists $\sigma \in G$ such that

$$\sigma(\alpha\zeta_2) = \alpha\zeta_2, \quad \sigma(\alpha\zeta_1) = \alpha, \quad \sigma(\alpha) = \alpha\zeta_1.$$

Therefore, $\sigma(\alpha) = \alpha\zeta_1$ and $\sigma^2(\alpha) = \alpha$. Since $\{\sigma \in G \mid \sigma(\alpha\zeta_1) = \alpha\zeta_1\} \neq \{\text{Id}\}$, there exists $\tau \in G$ such that $\tau(\alpha) = \alpha\zeta_2$ and $\tau^2(\alpha) = \alpha$. The conditions $\sigma^2(\alpha) = \tau^2(\alpha) = \alpha$ imply that σ, τ coincide in $\mathbb{Q}(\mu_m)$ with the complex conjugation. Thus $(\sigma \circ \tau)(\alpha) = \alpha\zeta_1\zeta_2^{-1}$. Since $\zeta_1\zeta_2^{-1} \in \{1, \zeta_1, \zeta_2\}$ and $\zeta_1 \notin \{1, \zeta_2\}$, we have that $\zeta_1 = \zeta_2^2$. Using $\tau \circ \sigma$, we obtain that $\zeta_2 = \zeta_1^2$. Thus, $\zeta_1, \zeta_2 \in \mu_3$ and $m = 3$.

ii) $H = \{\text{Id}\}$. In this case, $\tilde{K} = K$. The field $\mathbb{Q}(\mu_m)$ is totally imaginary because m is odd, and thus, $[\mathbb{Q}(\mu_m) : \mathbb{Q}]$ can only be equal to 6 or 2. Therefore, $K = \mathbb{Q}(\mu_7)$ or $m = 3$.

If $m = 3$ then $P(X) = (X^3 - \alpha^3)(X^3 - \bar{\alpha}^3) = X^6 + aX^3 + q^3$. It is clear that if $P(X) = X^6 + aX^3 + q^3$ then $\mathbb{Q}(\alpha^3) \subsetneq \mathbb{Q}(\alpha)$. ■

4.2. Example. We consider the modular curves $X_0(41)/\mathbb{Q}$, $X_0(41)/\mathbb{F}_3$, which have genus 3. Let A denote the jacobian of $X_0(41)/\mathbb{F}_3$.

From the tables of Wada, we see that the characteristic polynomial of the Hecke operator T_3 acting in $S_2(X_0(41))$ is $Q(X) = X^3 - 4X + 2$, which is \mathbb{Q} -irreducible. We consider the natural action of T_3 as endomorphism of $J_0(41)$, the jacobian of $X_0(41)$, and its (mod 3)-reduction, \tilde{T}_3 , as endomorphism of A . The \mathbb{Q} -irreducible polynomial of \tilde{T}_3 acting in $\Omega_1(A)$ is $Q(X)$.

The real field $L = \mathbb{Q}(\tilde{T}_3)$ has discriminant $2^2 \cdot 37$ and, thus, $L \not\subset \mathbb{Q}(\mu_7)$. The congruence of Eichler-Shimura establishes that $\tilde{T}_3 = \varphi + \varphi'$. Then $\mathbb{Q}(\varphi)/L$ is an imaginary quadratic extension and the \mathbb{Q} -irreducible polynomial of φ is

$$P(X) = X^3Q(X + 3/X) = X^6 + 5X^4 + 2X^3 + 15X^2 + 27.$$

By 3.1 ii), $r(A) = 3$, because the (mod 3)-reduced polynomial $Q(x)$ has three non zero roots. Since A is defined over \mathbb{F}_3 , then $e = 1$ and $\text{End}_{\mathbb{F}_3}^0(A) = \mathbb{Q}(\varphi)$.

Let $\alpha := 3\varphi$, which is a Weil 3^3 -number. We have that $\mathbb{Q}(\alpha^m) = \mathbb{Q}(\varphi^m)$ for all positive integers m . Let B/\mathbb{F}_{27} be the abelian variety associated to α . It has $r(B) = 0$, by 3.2 ii). The prime 3 is inert in L and does not ramify in $\mathbb{Q}(\alpha)$. The ideal (3) is not prime in $\mathbb{Q}(\alpha)$ because $r(A) \neq 0$. Then, we have that $(3) = \wp\wp^c$ with $f_\wp = f_{\wp^c} = 3$ in $\mathbb{Q}(\alpha)$. Thus, the Brauer periode e of $\text{End}_{\mathbb{F}_{27}}^0(B)$ is 1. Therefore, $\dim B = 3$ and $\text{End}_{\mathbb{F}_{27}}^0(B) = \mathbb{Q}(\alpha)$.

Since $P(X)$ is not of type $X^6 + aX^3 + 3^3$ and $\mathbb{Q}(\varphi) \neq \mathbb{Q}(\mu_7)$, we have by 4.1 that $\mathbb{Q}(\varphi) = \mathbb{Q}(\varphi^m)$, for all positive integers m . Thus, A and B are absolutely simple and $\text{End}^0(A)$, $\text{End}^0(B)$ are isomorphic to $\mathbb{Q}(\varphi)$.

References

- [Ba-Go 97] P. BAYER AND J. GONZÁLEZ, On the Hasse-Witt invariants of modular curves, *Experiment. Math.* **6** (1997), 57–76.
- [De 41] M. DEURING, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Univ. Hamburg* **14** (1941), 197–272.
- [Go 97] J. GONZÁLEZ, Hasse-Witt matrices for the Fermat curves of prime degree, *Tôhoku Math. J.* **49** (1997), 149–163.
- [Ha 34] H. HASSE, Existenz separabler zyklischer unverzweigter Erweiterungskörpern vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p , *J. Reine Angew. Math.* **172** (1934), 77–85.
- [Ha-Wi 36] H. HASSE AND E. WITT, Zyklische unverzweigte Erweiterungskörpern vom Primzahlgrade p über einem algebraischen Funktionenkörpern der Charakteristik p , *Monatsh. Math. Phys.* **43** (1936), 477–492.
- [Ma 65] J. I. MANIN, The Hasse-Witt matrix of an algebraic curve, *Amer. Math. Soc. Transl. Ser.* **45** (1965), 245–264.
- [Oo 87] F. OORT, Endomorphism Algebras of Abelian Varieties, Algebraic Geometry and Commutative Algebra, in honour of M. Nagata **2** (1987), 469–502.
- [Se 58] J. P. SERRE, Sur la topologie des variétés algébriques en caractéristique p , *Symp. Int. Top. Alg.*, México, p. 24–53, in “*Œuvres*,” vol. I, Springer.
- [St 79] H. STICHTENOTH, Die Hasse-Witt-Invariante eines Kongruenzfunktionenkörpers, *Arch. Math.* **33** (1979), 357–360.
- [Ta 66] J. TATE, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134–144.
- [Ta 68] J. TATE, Classes d’isogénie des variétés abéliennes sur un corps fini (d’après T. Honda), *Sém. Bourbaki* (1968/69), 95–110.
- [Wa 69] W. C. WATERHOUSE, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.* **2** (1969), 521–560.

- [Yu78] N. YUI, On the Jacobian varieties of hyperelliptic curves, *J. Algebra* **52** (1978), 378–410.

Departament de Matemàtica Aplicada i Telemàtica
Escola Universitària Politècnica de Vilanova i la Geltrú
Av. Victor Balaguer s/n
Vilanova i la Geltrú 08800
SPAIN

e-mail: josepg@mat.upc.es

Primera versió rebuda el 21 de gener de 1997,
darrera versió rebuda el 3 d'abril de 1997